Amendments to the Claims:

1 – 197. (Canceled)

198. (Currently Amended) A system for transferring items having value in a computer network comprising:

a plurality of user terminals coupled to a computer network;

a database system coupled to said network and remote from said plurality of user terminals for storing information about one or more users using said plurality of user terminals; and

a server system coupled to said network, said server system comprising cryptographic capabilities for transferring an item having value utilizing said information stored in said database system, wherein said server system is configured to continue verifying authentication over time while processing a request to transfer said item having value and to terminate said transfer of said item having value if said authentication is not continuously verified while said request is being processed, said continuous verification comprising the exchange of continuously changing messages.

199-202. (Canceled)

203. (Previously Presented) The system of claim 198, wherein said server system comprising said cryptographic capabilities further comprises a cryptographic device that generates a digital signature in response to a user request for printing said item having value.

204. (Previously Presented) The system of claim 198, wherein said server system comprising said cryptographic capabilities further comprises a cryptographic device that encrypts the requested information in response to a user request for printing said item having value.

205-212. (Canceled)

213. (Previously Presented) The system of claim 198, wherein said cryptographic capabilities comprise a cryptographic device that protects data using a stored secret.

214. (Previously Presented) The system of claim 213, wherein said secret is a password.

215. (Canceled)

216. (Currently Amended) A method for secure processing of items having value in a computer network comprising a plurality of user terminals comprising:

storing information about one or more users using a plurality of user terminals in a database system coupled to a network and remote from said plurality of user terminals; and

performing secure functions for an item having value utilizing said information stored in said database system to execute cryptographic capabilities remote from said plurality of user terminals;

continuing to verify authentication over time during performance of said secure functions for said item having value;

terminating said performance of secure functions for said item having value if said authentication is not continuously verified while said secure functions are being performed, said continuous verification comprising the exchange of continuously changing messages.

217-218. (Canceled)

219. (Previously Presented) The method of claim 216 further comprising authenticating the identity of each user.

220. (Previously Presented) The method of claim 219 further comprising verifying that the identified user is authorized to print said item having value.

221. (Canceled)

222. (Previously Presented) The method of claim 216, wherein said cryptographic capabilities are provided by a cryptographic device configured to generate a digital signature in response to a user request for printing said item having value.

223. (Previously Presented) The method of claim 216, wherein said cryptographic capabilities are provided by a cryptographic device configured to encrypt the requested information in response to a user request for printing said item having value.

224-240. (Canceled)

241. (Previously Presented) The system of claim 198, wherein said server system comprising said cryptographic capabilities further comprises a cryptographic device that encrypts the requested information in response to a user request for transferring said item having value.

242. (Previously Presented) The method of claim 219 further comprising verifying that the identified user is authorized to transfer said item having value.

243. (Previously Presented) The method of claim 216, wherein said cryptographic capabilities are configured to encrypt the requested information in response to a user request for transferring said item having value.